



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

ml

| | | | | |
|---|-------------|----------------------|---------------------------------|------------------------|
| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
| 10/613,636 | 07/03/2003 | Bhargava K. Yenduri | SUNMP459 | 4610 |
| 32291 7590 09/26/2007 MARTINE PENILLA & GENCARELLA, LLP 710 LAKEWAY DRIVE SUITE 200 SUNNYVALE, CA 94085 | | | EXAMINER HOMAYOUNMEHR, FARID | |
| | | | ART UNIT 2132 | PAPER NUMBER |
| | | | MAIL DATE 09/26/2007 | DELIVERY MODE PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/613,636

Applicant(s)

YENDURI, BHARGAVA K.

Examiner

Farid Homayounmehr

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11 July 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1, 3, 4, 9-11, 25, 27, 29 and 30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1, 3, 4, 9-11, 25, 27, 29 and 30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is responsive to communications: application, filed 7/3/2003; amendment filed 7/11/2007.
2. Claims 1-36 were pending in the case.
3. Claims 2, 5-8, 12-24, 26, 28, 31-36 were cancelled by the applicant.

Response to Arguments

4. Applicant has amended claim 1 to include the limitations of claims 5-8. In view of the amendment, applicant argues: "The Office's notice taken in section 6.1 of the Office Action, regarding signature verification protocols being well know is traversed. Although encryption technology is not proposed to be new, it is the way and form of its claimed use, in combination with the other claim elements, which are regarded to be inventive." However, applicant does not explain what is the specific way and form of the claimed use of encryption, and how this specific way distinguishes the invention from the prior art. There is no explanation on why it would not be obvious to the one skilled in art to use public and private keys to perform encryption within the framework of the claimed invention. The cited reference teaches the elements of the claimed invention, including kernel modules containing signature information. The only element that is not explicitly

Art Unit: 2132

taught by the reference is use of public and private keys to create signature information. As admitted by the applicant, the encryption technology used in creation of the signatures is not proposed to be new. Therefore, it would have been obvious to the one skilled in art to use public and private keys to create the signature information contained in the cited prior art's kernel modules.

Applicant further argues: "Specifically, the claims are directed toward a system that includes a kernel module signature verification system that verifies kernel module signature information of each kernel module as they are loaded onto the system--not somewhere on the network."

However, LKM agents verify the modules that are loaded onto the exemplified system too. As shown in paragraph 148, the agents verify the signatures of suspicious loadable kernel modules. The kernel modules are to be loaded onto the system.

Applicant further argues that the claimed invention includes both a kernel cryptographic framework and a kernel cryptographic framework daemon. However, inclusion of both a kernel cryptographic framework and a kernel cryptographic framework daemon were part of dependent claim limitations, which is taught by Rowland as reflected in the corresponding claim rejection.

Applicant also argues that the claimed invention also includes a kernel cryptographic framework that retrieves pathname information of signatures when the kernels attempt to load up. However, inclusion of a kernel cryptographic framework that retrieves

Art Unit: 2132

pathname information of signatures when the kernels attempt to load up was part of original dependent claim 8, which is taught by Rowland as reflected in the rejection of claim 8.

Based on the discussion above, applicant's argument relative to allowability of the pending claims is found non persuasive.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1, 3, 4, 9-11, 25, 27, 29 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rowland (US Patent Application Publication No. 2002/0129264 A1, filed January 10, 2002).

6.1. As per claim 1, Rowland is directed to a computer system comprising: a processor; a memory storage unit; an operating system comprising a kernel, said kernel comprising a plurality of kernel modules, said kernel modules comprising signature information; and a kernel module signature verification system for verifying said kernel module signature information of each of said plurality of kernel modules as said plurality

Art Unit: 2132

of kernel modules are loaded into said kernel (paragraph 149 describes a Loadable Kernel Module Agent 1306, which is an agent looking for loadable kernels and verifies their validity. As shown in Fig. 13, item 1306 is one of the agents in the group of Mobile Autonomous Code (MAC) Security Agents. Another one of the MAC agents is Known Intrusion Agent 1305 (paragraph 148), which uses signatures to identify intrusions such as suspect loadable kernel modules), wherein said kernel module signature information is generated via a public key and a private key compilation in said kernel module (use of public and private keys to create a signature verification protocol is well-known in the art) said kernel module signature verification system includes (a) a kernel cryptographic framework for verifying said kernel module signature information (paragraph 132) (b) a kernel cryptographic framework daemon for (i) performing verification lookup operations of signature information provided to said kernel cryptographic framework in said kernel (paragraph 153 shows use of system daemons to run a software process. Rowland also teaches verification of signature modules, which includes signature lookup. It would have been obvious to use a daemon to perform signature verifications, as a daemon is just a process that runs in the background and performs a specified operation at predefined times or in response to certain events (see <http://www.webopedia.com/TERM/D/daemon.html>)) (ii) performing module verification of said plurality of kernel modules (as mentioned before, Rowland teaches module verification by verifying the signature information), wherein said kernel cryptographic framework retrieves pathname information of said signature information for each of said plurality of kernel modules when said plurality of kernel modules attempt to load up to

Art Unit: 2132

said kernel to perform cryptographic operations (retrieving the pathname information is part of a typical access process in a computer. When the signature is fetched from the memory to the cryptographic process, it is accessed by its pathname).

6.2. Claims 2, 5-8, 12-24, 26, 28, 31-36 have been cancelled by the applicant.

6.3. As per claims 3 and 4, Rowland is directed to the computer system of claim 1, wherein said kernel module signature information comprises signature length data unique to each of said plurality of kernel modules, said signature length or size data used by said kernel module signature verification system in uniquely identifying each of said plurality of kernel modules (the signature verification process generates the signature of data and compares it with the signature. The generated signature and the signature must be identical, which means the length and size of the generated signature and the signature must also be identical).

6.4. As per claim 9, Rowland is directed to the computer system of claim 8, wherein said kernel cryptographic framework comprises a cryptographic service provider registration unit for registering each of said plurality of kernel modules wishing to provide cryptographic services in said kernel (per paragraph 29, all agents and processes of Rowland register with a module that oversees their operation).

Art Unit: 2132

6.5. As per claim 10, Rowland is directed to the computer system of claim 9, wherein said kernel cryptographic framework further comprises a intra-kernel communication unit for enabling communications between said kernel cryptographic framework and said kernel cryptographic framework daemon (paragraph 29 suggests a Master Control Process which is a communication unit allowing elements of the system to communicate with one another.).

6.6. As per claim 11, Rowland is directed to the computer system of claim 10, wherein said kernel cryptographic framework further comprises a data structure unit for storing said kernel module signature information (Rowland agents access to many different kinds of data, including signature data. Use of datastructures in computer systems to provide data to processes is well-known in the art).

6.7. Limitations of claims 25, 27, and 29 are substantially the same as claims 1-11 above.

6.8. As per claim 30, Rowland is directed to the computer operating system of claim 22, wherein said kernel cryptographic framework and said kernel cryptographic framework daemon communicate via a plurality of input/output control commands (paragraphs 29-31 describes how handlers communicate with one another to exchange messages. The messages contain commands to initiate the functionality of each handler).

Conclusion

7. **THIS ACTION IS MADE FINAL**, as no new ground of rejection is included. See MPEP § 7.39. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571) 272-3739. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

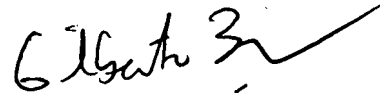
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

Art Unit: 2132

published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

9/18/07



GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100